Going it alone: The causes and consequences of U.S. extraterritorial counterproliferation enforcement

Published in *Contemporary Security Policy*, 2019
https://doi.org/10.1080/13523260.2019.1595882

Aaron Arnold, Belfer Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University, USA
Daniel Salisbury, Centre for Science and Security Studies, Department of War Studies, King's College London, UK

Abstract:

In 2004, the United Nations Security Council adopted resolution 1540, which acknowledged the non-state acquisition of weapons of mass destruction as a security threat and called on member states to implement "appropriate effective" domestic trade controls. The United States, however, has both promoted the multilateral implementation of international trade controls but has also increasingly resorted to extraterritorial enforcement of its counterproliferation rules. How can a multilateral, norms-based international regime like 1540 contend with extraterritorial enforcement based on national interests? We argue that increased U.S. extraterritorial counterproliferation policies are a consequence of the inconsistent implementation of resolution 1540, adaptive and resilient proliferation networks, and a history of expanding legal interpretations of jurisdiction. We find that while U.S. extraterritorial enforcement can effectively disrupt networks hiding in overseas jurisdictions, doing so creates disincentives for states to implement 1540 obligations and undermines broader nonproliferation objectives.

Keywords

counterproliferation; extraterritoriality; illicit trade; export controls; proliferation networks

Acknowledgements
None

Funding information
None

Disclosure statement
No potential conflict of interest has been reported by the authors.

Notes on contributors

Aaron Arnold is a fellow with the Project on Managing the Atom at Harvard Kennedy School's Belfer Center. His current work focuses on trade controls for preventing WMD proliferation. Prior to his current appointment, Aaron spent nine years as a non-proliferation and counter-proliferation subject matter expert at the U.S. Department of Defense and U.S. Justice Department, where he specialized in WMD counter-proliferation investigations and operations, with an emphasis on threat finance and sanctions evasion. Aaron holds a PhD and MPP in public policy and national security from George Mason University and a BA in international relations from Virginia Tech.

Daniel Salisbury is a Research Fellow at the Centre for Science and Security Studies (CSSS) within the Department of War Studies at King's College London. Daniel joined CSSS in July 2018 from the Harvard Kennedy School's Belfer Center for Science and International Affairs where he was a Stanton Nuclear Security Postdoctoral Fellow. Previously he was a Postdoctoral Fellow at the James Martin Center for Nonproliferation Studies (CNS) at the Middlebury Institute of International Studies at Monterey, a Research Associate at CSSS, and a Research Assistant at the International Institute for Strategic Studies (IISS).

In 2004, the United Nations (UN) Security Council adopted Resolution 1540, which obligates member states to prevent non-state actors from acquiring, developing, or using weapons of mass destruction (WMD) and their means of delivery. This decision was significant for several reasons. First, the Security Council adopted the resolution under Chapter VII of the UN Charter—meaning that compliance with the resolution's requirements is mandatory, whereas past treaties and regimes were voluntary. Second, the resolution not only recognized that the *ad hoc* system of global WMD-related supply-side controls, at that time, was inadequate to address the threats posed by non-state actors but also emphasized the need for cooperation and coordination at both national and international levels. Since its adoption, the resolution has become a cornerstone of the global nonproliferation regime; addressing important gaps in global supply-side controls.

Almost fifteen years after the adoption of United Nations Security Council Resolution (UNSCR) 1540, and despite the resolution's legally-binding obligations, significant technical outreach, training, and capacity-building efforts, overall implementation and enforcement of the resolution's provisions continue to vary significantly by country. Consequently, proliferators have exploited implementation variance in order to illicitly procure dual-use goods and technologies (i.e., goods that have both commercial and military or WMD applications) from the global marketplace. North Korea, for example, has made significant progress toward its WMD and missile programs by exploiting weak export controls in third-party countries in order to illegally obtain export-controlled goods and technologies. Without an international mechanism to enforce compliance with the resolution, advancing the UNSCR 1540 agenda has tended to be driven forwards by bilateral assistance programs–and particularly those funded by the United States.

While promoting greater global implementation of international supply-side controls, the United States has simultaneously taken an increasingly extraterritorial approach to counterproliferation enforcement.[1] Extraterritorial enforcement is the practice of one country imposing its domestic laws inside the jurisdiction of another country, but without seeking permission. Since 2005 the United States has resorted to expansive extraterritorial methods, which take advantage of unique authorities and status within global financial and economic systems. These methods have included autonomous sanctions, regulatory enforcement actions, civil and criminal asset forfeitures, and extradition arrangements. This raises an interesting question: how does a norms-based

---

1

 In this article, we define counterproliferation as the national law enforcement, regulatory, intelligence, and defense policies that address WMD-related proliferation security threats (Carter, 2004). For our analysis, we focus exclusively on U.S. law enforcement and regulatory actions, which are the most publicly visible. That is, we do not consider the range of intelligence and defense-related enforcement systems, which are far less visible.

international regime contend with national interest-based, extraterritorial enforcement actions?

Through a review of the scholarship, U.S. court documents, and interviews with law enforcement specialists we aim to answer two key questions. First, what are the factors driving U.S. extraterritorial enforcement? Second, what are the knock-on effects and implications for global supply-side controls? To this end, this article aims to not only contribute to emerging scholarship on enforcement of WMD supply-side controls but also adds a new dimension by introducing the concept of extraterritoriality. Within this context, we highlight the emerging tension between an international approach to controlling the spread of proliferation-sensitive goods and technologies and the costs of pursuing national security interests vis-à-vis extraterritorial enforcement practices. This tension, we argue, is likely to result in U.S. counterproliferation tools becoming less effective in the long-term and may undermine broader nonproliferation objectives.

The supply side of WMD counterproliferation

The evolution of the U.S. approach to supply-side controls discussed in this article builds on two sub-genres of the proliferation scholarship: First, the literature on *how* states go about developing WMD; and second, the literature on supply-side controls, or how other states seek to prevent proliferators from obtaining WMD technologies. Research, by far, has focused more on the demand-side than the supply-side of WMD proliferation–essentially addressing *why* states seek WMD. Sagan (1997), for example, provided a seminal typology of states' demand for WMD, based on existential security threats, a function of domestic politics, or as a desire for national or international prestige. Although there is a robust and active scholarship on why states' pursue WMD, there still lacks any generalizable or unifying theory. As Narang (2016) puts it, "[k]nowing why states might pursue nuclear weapons … does not explain how they might do so" (p. 112).

Only more recently have scholars started to consider the nuance of *how* states build their WMD programs. In general, these studies have contributed to a more nuanced view of the range of political pathways to a bomb, as well as the processes that states use to acquire necessary skills and technologies. The assumption, of course, is that understanding *how* will lead to better inhibition approaches, from forming and reinforcing nonproliferation norms to coercive diplomacy (Gavin, 2015).

The focus of this work considering *how* states proliferate has varied in scope. Historically, from a policy perspective, states have viewed clandestine state-to-state transfers and black-market activity as the primary way that states acquire sensitive technologies to build WMD programs (Kemp, 2017). Consequently, supply-side controls (e.g., trade controls) emerged as a key nonproliferation policy. Kemp (2014), for example, argues that since the beginning of the atomic age, policymakers have wrongly believed that technological barriers to building a nuclear weapon presented an adequate

obstacle to further proliferation. Whether or not Kemp's argument is correct, domestic and international responses to states' demand for WMD have emphasized the need to control the supply of WMD-related goods and technologies. In the early 2000s, however, it became apparent that global supply-side controls failed to address a new WMD proliferation threat—the rise of the non-state actor.

One of the most important contributions to scholarship on states' proliferation strategies is the recognition that more recent nuclear proliferators and aspirants have pursued pathways that are fundamentally different than the first nuclear weapons states. Einhorn (2006), for example, highlights how the United States, Soviet Union, United Kingdom, France, and China, "... each developed, weaponized, tested, produced, and deployed nuclear weapons" as soon as possible" (Einhorn, 2006, p. 495). Subsequent states that acquired nuclear weapons capabilities (or those that attempted to) took a variety of approaches—some incremental, hedging against running afoul of nonproliferation norms, while other more covert.

Much of the early work on proliferation pathways assumed that state-to-state technology transfers, particularly sharing nuclear energy, posed a significant risk. With regards to civil nuclear assistance, Fuhrmann (2012, 2009; see also Holdren, 1983) has argued that peaceful assistance ultimately raises the risk of nuclear proliferation. Many believed that sharing nuclear energy technology would lower a state's expected costs to build a bomb, would create an "irresistible temptation" to proliferate, and would provide technical and political cover for states to acquire enrichment or other weapons-related technologies (Holdren, 1983). Others have argued that states share sensitive technologies with non-nuclear weapons states for strategic advantage (Kroenig, 2010).

New work, however, questions this conventional wisdom. As Miller (2017) astutely points out, however, much of the conventional wisdom about the relationships between civilian energy programs and nuclear weapons proliferation is incorrect. Instead, he finds that countries with nuclear energy programs are not more likely to proliferate, due in part to increased chances of detection and the costs from potential sanctions.

As the A. Q. Khan network unraveled, fears emerged over "second-tier" proliferation. That is, states or entities within states who sell proliferation-sensitive goods and technologies on the open market (Braun & Chyba, 2004). Pakistan, for example, was ultimately the source of sensitive technology that made its way into North Korea, Iran, and Libya. By the same token, North Korea has proliferated ballistic missile technology to Iran, Libya, and Pakistan. While some have argued that intangibles, like tacit knowledge, still present a significant barrier to building a nuclear weapon (Montgomery, 2005), others have argued the necessary technology is more readily available that previously thought. Kemp (2014, 2017), for example, argues that the notion that technically weak states proliferate through black-market activities or state-to-state transfers is incorrect. Instead, he shows that increased information availability about

centrifuge technology likely had a greater effect on centrifuge production than the A. Q. Khan network.

In a recent article, Narang (2016) introduced a typology of states' strategies to acquire nuclear weapons: hedging, sprinting, hiding, and sheltered pursuit. According to Narang, a hedger "refrains from actively developing nuclear weapons but has not explicitly forsworn the option, putting the pieces in place for a future nuclear weapons program" (p. 117). States that "sprint" seek to develop nuclear capabilities as quickly as possible, but do not necessarily attempt to hide their efforts. Conversely, states that are "hiders" try to avoid detection by other states. Finally, states that pursue a "sheltered pursuit" strategy exploit the advantage provided by a major power to pursue nuclear capability (Narang, 2016, p. 122). Of course, the specific strategy or combination of strategies that a state pursue, according to Narang, is a function of external and domestic political environments.

One implication of Narang (2016) and Einhorn's (2006) work is that states which pursue covert WMD programs may lack the indigenous expertise and thus left to buy, barter, or steal the necessary expertise and equipment. Whereas plutonium reprocessing may draw international scrutiny, for example, using centrifuges to enrich uranium may be done in a way to obscure or hide true intentions. Consequently, states may be left to gray and black markets to acquire technologies that fall below export-control thresholds and trigger lists (Einhorn 2006, p. 493). Iran, for example, pursued a clandestine weapons program that at least initially relied on centrifuges and design information from the A.Q. Khan network. While the covert program ended in 2003, important technical aspects of the program continued as part of the country's civil nuclear program—relying on dual-use goods and technologies from foreign suppliers. Libya also attempted to covertly buy turn-key enrichment capabilities from the Khan network. In the past, North Korea has sourced advanced materials from foreign suppliers.

Interestingly, while emerging scholarship recognizes the unique challenges of detecting a states' covert WMD programs and the importance of supply-side controls, there is still only a nascent body of literature that addresses the processes of illicit procurement and its implications for policymakers. A. Q. Khan's nuclear proliferation network brought to light the challenges and limitations of existing export control regimes. His network employed layers of intermediaries, suppliers, and financiers that stretched from Europe and Southeast Asia to the Middle East in order to sell nuclear enrichment technologies, weapons plans, and other dual-use goods to Iran, Libya, and North Korea (Albright & Hinderstein, 2005). As Khan's network unraveled, it was apparent that global export control regimes—at the time—were unprepared to deal with non-state WMD proliferation. Existing export control regimes, like the Nuclear Suppliers Group, the Australia Group, and the Missile Technology Control Regime, were each informal, multilateral agreements between supplier states that provided guidelines and established norms for the supply of proliferation-sensitive technologies. These agreements, although

non-legally binding, helped supplier states to fulfill their obligations spelled out in international nonproliferation treaties, like the Nonproliferation Treaty, the Chemical Weapons Convention, and the Biological Weapons Convention. These regimes, however, were not legally-binding, failed to keep pace with rapid globalization and the spread of dual-use goods and technologies, and ignored the emerging role of the non-state actor in WMD proliferation.

By May 2003, the Bush administration had started to explore options to address non-state WMD proliferation. One of the first efforts was the U.S.-led Proliferation Security Initiative (PSI), which is a non-binding agreement between members that outlined a broad set of principles to interdict shipments potentially related to WMD trafficking. Initially only 40 members, PSI membership now totals 105. As Tobey (2018, p. 18) points out, however, although PSI improved coordination and communication between international counterproliferation efforts, it did not address several legal challenges. Namely, most states did not have adequate domestic legislation that criminalized activities associated with non-state WMD proliferation. Some Bush administration officials believed that states should treat WMD trafficking the same way as piracy on the high seas (Sokolski, 2003, p. 9). That is, states have the right to address piracy irrespective of national jurisdiction. Thus, from the beginning, there was a tension between recognizing the need for multilateral approaches and domestic pressures to take more unilateral actions.

Eventually, Bush administration officials moved to put forward a UN resolution that would mandate countries to address WMD proliferation threats by requiring states to criminalize the proliferation of WMD and to put into place national export control systems. The UN Security Council adopted Resolution 1540 in April 2004—a legally-binding resolution that recognized the need to address the problem of non-state actors, like terrorist groups and trafficking networks. Specifically, UNSCR 1540 requires that states, "adopt and enforce appropriate effective laws which prohibit any non-State actor to manufacture, acquire, possess, develop, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery" (United Nations Security Council, 2004a, paragraph 2). UNSCR 1540 effectively "replaces a de facto norm of behavior with a de jure legal requirement" (Stinnett, Early, Horne, & Karreth, 2011, p. 312).

At the time of the resolution's adoption, then President of the UN Security Council, Gunter Pleuger, noted that the "... proactive cooperation of all Member states, the public, private industry, and international agencies was a prerequisite for its success." He went on to say that, "In case of any lack in [the Resolution's] implementation, the resolution did not foresee any unilateral enforcement measures" (as cited in United Nations Security Council, 2004b). Thus from the onset, many criticized the conceptual inconsistencies between the resolution's legal underpinning and the flexibility with respect to implementation in its operative paragraphs. Although the Security Council had the opportunity to choose an "enforcement approach" to governance, Heupel (2008, p.

22) argues that doing so would have ultimately undermined confidence. As Early, Nance, and Cottrell (2017) note, "Enforcement as a collective policy of the Council seems off the agenda entirely. Hardly the command-and-control, top-down model of regulation that its extraordinary legal foundation seemed to foreshadow, the resolution establishes standards but allows for flexibility in how states meet them" (p. 96).

In fact, there is a significant vein of scholarship that is cautiously optimistic about the resolution's progress and the success of a soft-governance approach. Despite concerns over the resolutions vague language and the possibility for an even more fragmented international system of national export controls, bilateral assistance has helped the regime to overcome many the resolution's initial criticisms. Since 2004, states' implementation of UNSCR 1540 requirements have varied significantly, and according to the most recent UN implementation assessment, many states have yet to adhere to all of the mandates fully. One issue is that UNSCR 1540 does not prescribe specific legislation, but instead leaves it up to each member state to implement its obligations consistent with its own national political and economic systems. The last assessment of 1540 implementation, which occurred in 2016, found that while states have made progress overall, several gaps remain. While seventy-percent of member states have implemented some national-level export control system for nuclear-related goods and technologies, less than fifty-percent of states have published controls lists, only thirty-percent of states have catch-all provisions, and about forty percent of states address transshipment (United Nations Security Council, 2016, pp. 61–70).

There are two general explanations for states' failures to comply with 1540 obligations fully. The first, suggests that states see export controls as self-limiting and potentially harmful to economic and security interests. The second approach sees compliance failures as a function of limited capacity and capability—rather than political will. In an early study of national export control systems, Cupitt, Grillot, and Murayama (2001) proposed a framework based on an economic-rationalist perspective to describe the conditions when states are likely to implement internationally compatible export controls. The framework explained why states implement export control systems in terms of maximizing the political and economic benefits of belonging to a liberal international community. The economic costs—particularly resource constraint—and political costs of administering a national export control system accounts for a "considerable portion of the policy variance" between countries (p. 74), rather than the particular government's perception of external security threats posed by WMD-related illicit trade and proliferation.

In a more recent study, Stinnett et al. (2011) draw from theories of international law to discuss states' compliance with UNSCR 1540 from two perspectives: enforcement and capacity. Whereas the enforcement perspective explains compliance as a consequence of national interest and external pressures (Downs, Rocke, & Barsoom, 1996), the capacity perspective emphasizes limitations in the technical and bureaucratic

capacities of governments (Chayes & Chayes, 1993). In an analysis of thirty countries, the authors found significant evidence to support the limited capacity explanation for states' willingness to implement its UNSCR 1540 obligations (Stinnett et al., 2011, p. 309). Moreover, the authors found no support for the hypothesis that states with economies that rely heavily on exports would have greater economic incentives not to implement 1540 obligations or the hypothesis that strategic partnerships with the United States are associated with "more aggressive nonproliferation efforts" (p. 323). These findings are consistent with an early study of UNSCR 1540 compliance by Fuhrmann (2007), who argues that compliance is strongly associated with both political willingness and capacity.

Thus, from a governance perspective, non-compliance is easily addressed through bilateral and multilateral cooperative efforts. In the United States, for example, the State Department's Export Control and Related Border Security Program (EXBS) has provided technical assistance, training, and outreach to more than sixty countries with varying degrees of success. However, this approach is still inadequate to address non-compliant and non-cooperative states. In fact, the United States has taken coercive tactics when presented with egregious issues of non-compliance. For example, the United Arab Emirates and Malaysia both implemented national export legislation in 2007 and 2010, respectively, but only after the threat of penalties by the United States.[2]

We argue that as the United States publicly advocated for multilateral cooperation with respect to implementing and enforcing supply-side controls, policymakers began a concerted effort to expand extraterritorial methods to coerce non-compliant states and to disrupt overseas illicit procurement networks. In the next sections, we identify two factors that have significantly contributed to the United States' increased use of extraterritorial tools. First, global implementation of UNSCR 1540 obligations has been slow coming and varied and as consequence of these implementation shortfalls, transnational illicit procurement networks have been able to capitalize on governance and enforcement gaps between states. Second, over the last three decades, the United States has significantly expanded its view of jurisdiction, which in concert with new legislation after the September 11, 2001 terrorist attacks greatly expanded the arsenal of tools to use against those trafficking in WMD-related goods and technologies.

Adaptive transnational illicit procurement networks create jurisdictional hurdles

Illicit procurement networks—that is, the groups of intermediaries and middle responsible for procuring WMD-related goods and technologies--have featured prominently in recent cases of proliferation; helping proliferating states to obfuscate the

---

2

 For example, these included the risk of the UAE being designated a "Destination of Diversion Concern" under U.S. export control law, and the risk of Malaysia not being invited to Obama's first Nuclear Security Summit in 2010.

true end-user and evade potential detection and possible sanctions regimes. Iran and North Korea, for example, have consistently relied on transnational supplier networks to illicitly procure goods and technologies for use in their WMD and conventional military programs. Three characteristics of these networks make them particularly challenging for states and the UNSCR 1540 agenda to address: They operate in the grey market, are highly adaptable, and work across multiple jurisdictions.

Operating in the Grey Market

First, trafficking in dual-use goods and technologies is unlike many other types of transnational criminal activity because these illicit networks do not operate entirely on the "black market." Rather, they occupy a space somewhere in between legitimate markets and grey markets. Generally, illicit procurement networks must buy from a legitimate supplier. Doing so requires the network to employ legitimate financial, shipping, and licensing procedures—or deceive other actors that they are doing so. This means that at least one end of any given transaction will appear entirely legitimate to regulators and enforcement agencies.

Take, for example, the 2016 case of Sihai Cheng—a Chinese intermediary who illicitly procured thousands of export-controlled pressure sensors that ultimately made their way into Iran's nuclear enrichment program.[3] According to the U.S. criminal indictment and subsequent sentencing transcripts, between 2005 and 2012 Mr. Cheng established a series of front companies in order to pose as an end-user to receive the export-controlled parts from a U.S. manufacturer and supplier (U.S. District Court of Massachusetts, 2013). At the time, Cheng was working with the U.S. supplier's subsidiary, which was based in Shanghai. This allowed Mr. Cheng to hide his illicit activities within completely legitimate channels of trade. In other words, the pressure sensors were fully licensed for export to Mr. Cheng's front companies. From a detection and enforcement perspective, all of Mr. Cheng's intra-office transactions appeared completely legitimate.

3

 Pressure sensors, also commonly referred to as "pressure transducers," have a wide array of commercial uses, but can also be used to in gas centrifuges to convert natural uranium into enriched uranium.

Ability to Adapt

Second, illicit WMD procurement networks are not static groups of entities, but highly adaptable and can change their behavior to reflect environmental conditions– whether changing political and economic realities, or to evade evolving approaches to enforcement. The speeds at which illicit networks can adapt frequently outstrips the speed at which enforcement agencies can respond. While this important feature has received little attention in the literature on WMD procurement networks, others have covered similar problems of adaptive networks concerning other types of transnational crime and terrorism. Kenney (2007), for example, shows that narcotics trafficking networks and terrorism networks adapt to supply-side controls as a survival mechanism in order to counter and evade enforcement actions. Kenney writes, "At their best, supply-reduction programs have produced temporary ripples that quickly settle as traffickers establish alternative sources of supply, move their drug plantings and processing labs, invent new production methods, and create fresh transportation routes" (p. 2).

North Korea's illicit procurement and sanctions evasion networks have shown to be particularly adept at adapting to internal controls and evolving enforcement systems. The 2018 UN Panel of Experts report on North Korea, for example, notes that the country uses "increasingly sophisticated evasion practices" to undermine sanctions regimes (United Nations Security Council, 2018, p. 4). In a recent study, Park and Walsh (2016) argue that international sanctions have had the unintended consequence of actually improving Pyongyang's sanctions-busting capability. As international sanctions increase the cost of doing business for North Korea, the country adapts by paying its networks of middlemen and intermediaries higher commissions and fees—a process that monetizes risk (Park & Walsh, 2016, p. 32). These findings are broadly consistent with prior research on the unintended effects of sanctions and network adaptation (Andreas, 2005).

Transnational Networks

Third, this ability to adapt is also reflected in their operation across multiple jurisdictions around the world. The evolving geography of these networks as they respond to different political, legal, regulatory, and enforcement environments has been noted (Hastings, 2012). While often sourcing technology from industry in advanced economies, these networks often conduct their operations in "third country" hubs to obscure the end user and avoid enforcement action (Salisbury, 2019). These networks, therefore, exercise a type of "jurisdictional arbitrage"—picking jurisdictions which are less regulated and with a lower willingness or ability to enforce (Williams, 2001, p. 71). If corresponding national export control legislation and enforcement mechanisms do not

similarly adapt, procurement networks can exploit the resulting gaps (Arnold, 2017). These factors have made illicit procurement networks truly global in nature. One recent study indicated that in 2017, North Korea had offshore operations in fifty-two countries (Albright, Burkhard, Lach, & Stricker, 2018). Another noted that the country exploited more than 60 foreign jurisdictions in its WMD and military procurement efforts up to 2016 (King's College London, Project Alpha, 2016, p. 13). As a result, countering illicit networks has become a global game of "cat and mouse" or "whack-a-mole"—with each transfer playing out across several foreign jurisdictions, and interested national authorities struggling to keep up and act against these networks activities.

Given these three features of illicit WMD procurement networks—operating in grey markets, the ability to adapt rapidly, and choose jurisdictions—conventional approaches to supply-side controls, especially those mandated by UNSCR 1540, are insufficient. When it comes to non-cooperative jurisdictions, enforcement becomes all the more difficult. In these cases, it becomes more likely that countries, like the United States, will resort to extraterritorial measures.

The United States expands its jurisdiction across the globe

International interpretations of jurisdiction vary significantly. Most countries base their interpretation of jurisdiction on one or more of four general principles. The first principle defines jurisdiction in terms of geographic territory (Kelsen, 1945, p. 208). Over the last several decades, however, economic globalization and the rise of international non-governmental organizations have reduced the relevancy of a territory-oriented principle of jurisdiction in most cases (Alexander, 2009, p. 68; Slaughter, 1997). The most commonly adopted principle is the nationality principle, which extends jurisdiction over citizens no matter their geographic location. Some countries, like the United States and Canada, have interpreted the nationality principle in a rather broad context to include citizens, companies, and property. This includes foreign companies that are owned or operated by U.S. entities, but otherwise located abroad, as well as companies that may only be partially owned by U.S. entities.

The last two legal dimensions of jurisdiction are the protective and universal principles. The protective principle is based on the belief that sovereign states have the right to protect their economic and security interests (Alexander, 2009, p. 85). In this respect, claiming extraterritorial jurisdiction is consistent with international legal norms, but is substantively and arbitrarily defined by each state in terms of what constitutes a threat. Lastly, states may claim extraterritorial jurisdiction in order to enforce universal rights, which is mainly concerned with state violations of international law on slavery, piracy, and human rights.

Problems quickly emerge, however, when a citizen of one country violates the law or threatens the security and safety of nationals in a foreign country. Under these

circumstances, international norms have generally held that the extraterritorial application of domestic law must be through the consent of the state (i.e., the foreign jurisdiction). In practice, extraterritorial enforcement is conducted through multilateral or bilateral extradition agreements. Another issue arises when jurisdictional claims by one state create confusing or contradictory obligations for an individual or company headquartered in a foreign country. In other words, what happens when complying with one state's laws comes into conflict with another state's domestic laws?

In the United States, several legislative and regulatory changes between 1977 and 2001 significantly expanded the scope of jurisdiction and the scale of extraterritorial enforcement activities. In 1979, for example, Congress passed the Export Administration Act, which gives the president authority to regulate the import and export of goods for national security purposes. Because Congress failed to specify its intent as to what jurisdiction entailed, presidents have subsequently taken a rather broad interpretation to include property (Solensky, 1986, p. 126).

The most significant changes to U.S. extraterritorial policy occurred after the September 11, 2001 terrorist attacks. Congressional leaders determined that amendments to existing rules and regulations could help address jurisdictional gaps, especially when dealing with terrorist financing. Administrative and statutory reforms under the 2001 USA PATRIOT Act ushered in a new era of "financial warfare" that leveraged the strength of the U.S. financial system to address security threats ranging from terrorism and WMD proliferation to human rights violations and narcotics trafficking. According to Juan Zarate (2013), a former Bush administration Treasury official and one of the key architects of these strategies, "[t]he twenty-first century financial and commercial environment had its own ecosystem that could be leveraged uniquely to American interests" (p. 151). In other words, when it comes to global trade and commerce, the U.S. dollar remains the leading global reserve currency, as well as the preferred denomination for trade, which proved to be an opportune choke-point. The critical point of departure from past strategies rested in the administration's policy to leverage the global financial system to target specific actors. In a sense, this represented a significant expansion in the interpretation of jurisdiction, which previous administrations generally avoided.[4]

As the A.Q. Khan network began to unravel in 2003, the U.S. Department of the Treasury looked to its counter-terrorist financing playbook for strategies to block proliferators and would-be proliferators from financing their illicit activities. One of the

---

4

In 1982, for example, the French government ordered its largest oil and natural gas manufacturers to proceed with shipments to the Soviet Union in direct violations of U.S. sanctions—mainly as a protest to America's extraterritorial application of its domestic law. Amidst a rising tide of protests from key economic partners, President Reagan rolled back the extraterritorial dimensions of these sanctions (Perlow, 1983).

first tests came in September 2005, when the Financial Crimes Enforcement Network (FinCEN) declared a small Macanese-based bank—Banco Delta Asia—to be a "jurisdiction of primary money laundering concern" under Section 311 of the USA PATRIOT Act for substantially contributing to North Korea's illicit financial activities (U.S. Department of the Treasury, 2005).[5] Under this authority, FinCEN can require U.S. financial institutions to implement one or more "special measures" designed to deny bad actors access to the U.S. financial system. Such special measures can include maintaining certain detailed records, obtaining true beneficial ownership information, identifying correspondent customers, and the most serious, denying U.S. institutions from opening certain correspondent or pass-through accounts.[6] In addition to the designation under Section 311, U.S. authorities also froze $25 million linked to the North Korean regime.[7] The unintended effect of Banco Delta Asia's designation and the subsequent asset freeze was significant, swift, and widespread. Fearing damage to reputation and losing access to U.S. banking systems, financial institutions around the world cut ties with the Macanese bank almost overnight.

Although the U.S. Government has used Section 311 designations sparingly, they demonstrated the power of U.S. financial pressure and provided a template to target the financing of proliferation, as well as a means to disrupt illicit procurement activities and rogue regimes. In late 2016, for example, the Trump administration used the authorities to target North Korea's offshore banking networks—mainly located in China—which the regime used to maintain its illegal access to the global financial system. Under the 2016 ruling, U.S. authorities prohibited American banks from opening or maintaining any correspondent account with Bank of Dandong—a small China-based bank—or any

---

5

 Previous Section 311 designations were primarily related to terrorism or other types of transnational crime.

6

 Correspondent banking is when one bank carries out transactions on behalf of another bank - usually a foreign bank. These relationships allow a customer at one institution to quickly send a payment to a foreign bank. For example, Bank of China would settle a payment from an account holder at Bank of New York by debiting Bank of New York's correspondent account and credit its client. If, say, Bank of China and Bank of New York did not have a correspondent relationship, the transaction might need to go through multiple correspondent accounts at different banks (i.e., a correspondent network).

7

 The United States later allowed the $25 million to be unfrozen and transferred out of Banco Delta Asia to a Russian bank as part of diplomatic efforts to curb North Korea's nuclear activities in June 2007.

international bank that does so. Bank of Dandong held several accounts for Korea Mining Development Corporation (KOMID), which the United States and the United Nations sanctioned for being a primary exporter of goods and technologies relating to ballistic missiles and conventional arms.[8]

In order to address the financing of proliferation concerns more directly, President Bush signed Executive Order 13382 in June 2005, which provided the legal authority for the Department of State, in consultation with Department of the Treasury, to block assets and transactions of any individual or company.[9] Once Treasury Department adds an entity to its sanctions list, U.S. businesses are prohibited from engaging in any transactions—with few exceptions—and block (i.e., confiscate or freeze) any property or transaction within the United States.[10]

Even given the broad range and scope of the U.S. arsenal of financial weaponry, jurisdictional hurdles can still prove challenging. For example, North Korean illicit networks operating in foreign jurisdictions, like China, face little threat from U.S. regulatory and legal authorities—especially if the entities use small, regional banks with few ties to U.S. institutions. Recently, however, the U.S. Department of Justice has taken concerted steps to leverage national civil legal authorities to disrupt overseas networks that would otherwise be considered outside of U.S. legal jurisdiction.

The legal basis to leverage U.S. civil courts is quite clever. The International Emergency Economic Powers Act is also a predicate offense for money laundering—that is, intentionally hiding the proceeds from illicit activity. Thus, if a company or individual violates IEEPA, they could also be charged with a money laundering offense. Under U.S. law, money laundering includes both criminal *and* civil penalties. The most notable, of course, is asset forfeiture. The latter provides significant leverage for U.S. authorities to target the finances of overseas networks by employing a little-known provision of the USA PATRIOT Act.

8

 The U.S. government designated KOMID under executive orders 13382, 13687 in July 2005, and UNSCR 1718 (2006) in April 2009.

9

 The Executive Order states, "...engaged, or attempted to engage, in activities or transactions that have materially contributed to, or pose a risk of materially contributing to, the proliferation of weapons of mass destruction or their means of delivery (including missiles capable of delivering such weapons), including any efforts to manufacture, acquire, possess, develop, transport, transfer or use such items, by any person or foreign country of proliferation concern" ("Executive Order 13382," 2005).

10

 Some exceptions include academic exchanges, educational materials, humanitarian aid.

One of the key reforms in the USA PATRIOT Act was to amend U.S. forfeiture statutes to include interbank (i.e., correspondent) accounts.[11] In other words, prosecutors can indirectly seize proliferator assets held overseas by targeting the foreign bank's accounts in the United States. To date, however, U.S. prosecutors have been somewhat reluctant to fully leverage these authorities to target North Korean or Iranian illicit proceeds. There have been only five such instances.[12] The most recent cases of civil asset forfeiture involve targeting North Korea's networks of intermediaries and financiers that allow the regime to evade international sanctions and access the global financial system. In September 2016, U.S. prosecutors brought a civil case against Dandong Hongxiang Industrial Development (DHID) in the District of New Jersey for violating IEEPA and conspiracy to commit IEEPA violations.

According to the criminal complaint, Ma Xiaohong and her top executives established more than twenty-two front companies around the world to help North Korea's Kwangson Banking Corp., which was sanctioned in 2009 for its role in evading financial sanctions in order to facilitate dual-use procurement (U.S. District Court of New Jersey, 2016). Using shell companies registered in secrecy jurisdictions like Seychelles and the British Virgin Island, DHID acted as a payment processor for U.S. dollar-denominated transactions on behalf of North Korean banks. Under the civil forfeiture action, U.S. prosecutors seized $74 million from twenty-five separate bank accounts at several Chinese banks.[13] These banks ranged considerably in size from large national institutions to small regional banks. Most importantly, however, each held correspondent

---

11

 Explicitly the code states, "if funds are deposited into an account at a foreign bank, and that foreign bank has an interbank account in the United States with a covered financial institution...the funds shall be deemed to have been deposited into the interbank account in the United States, and any restraining order, seizure warrant, or arrest warrant *in rem* regarding the funds may be served on the covered financial institution, and funds in the interbank account, up to the value of the funds deposited into the account at the foreign bank, may be restrained, seized, or arrested" (The USA PATRIOT Act, 2001).

12

 Of the five civil cases, four have been against North Korean networks. These have included: Mingzheng International Trading Limited, Dandong Hongxiang Industrial Development, Velmur Management, and Dandong Chentai Trading Limited.

13

 These included China Merchants Bank, Shanghai Pudong Development Bank, Bank of Communications Co. of China, Bank of Dandong, China Construction Bank, Guangdong Development Bank, Industrial and Commercial Bank of China, Bank of Dalian, Bank of Jinzhou, Hua Xia Bank, and China Minsheng Banking Corporation.

relationships with U.S. institutions, where prosecutors were able to serve the seizure warrants.

Administrative innovations have also emerged in addition to targeted sanctions and legal actions. In March 2017, ZTE Corporation, China's largest telecommunications equipment manufacturer, agreed to $1.9 billion in criminal and civil penalties for illegally shipping U.S.-origin telecommunications equipment to Iran and North Korea (U.S. Department of Commerce, 2018a, 2018b). The most significant action, however, was not the criminal and civil penalty, but the seven-year suspended denial of export privileges. Meaning, if ZTE Corp. breached its agreements with prosecutors, the Department of Commerce would deny the company its ability to directly or indirectly import technology from the United States. Consequently, any U.S. person or company would be prohibited from transacting with ZTE for seven years— potentially upending a lucrative market worth billions and possibly even leading to the company's bankruptcy. In this context, the Department of Commerce leveraged its administrative authorities to coerce a major multi-national corporation— ultimately disrupting North Korea and Iran's ability to procure telecommunications equipment with U.S. origin components.[14] Thus far, ZTE Corp. is the only known instance where U.S. officials targeted a foreign company for sanctions violations using Department of Commerce administrative procedures.[15]

Taken together, it is clear U.S. extraterritorial approaches to counterproliferation are not the result of a singular policy decision, but a consequence of a change international security threat, the lack of an international mechanism to enforce 1540 implementation, and a history of expanding views on jurisdiction. In the next section, we conclude by exploring the potential challenges and consequences of the United States continuing to pursue unilateral and extraterritorial enforcement with respect to global nonproliferation goals and objectives.

14

 In April 2018, Department of Commerce Secretary Wilbur Ross revoked ZTE's suspended status and imposed a denial of export privileges order on ZTE for making false statements and misleading the U.S. Government during its negotiations in 2016. It is important to note, however, that the rationale for imposing the denial order was likely linked to a political dispute between the Trump administration and China over trade tariffs (Swanson, 2018).

15

 Controversy erupted in December 2018, when Canadian officials arrested a top executive at Huawei—a large Chinese telecommunications company—at the request of U.S. authorities. The United States accused the executive of violating U.S. unilateral sanctions against North Korea and Iran.

U.S. extraterritorial counterproliferation efforts: Challenges and consequences

Despite the perceived power of extraterritorial enforcement efforts, it is not clear whether such efforts are effective. To date, there has been no systematic analysis of whether extraterritorial tools are an effective or practical approach to countering proliferation networks. First, the number of cases that can be considered extraterritorial is rather small compared to the entire universe of proliferation-related cases. Second, because the number of cases is small, it is nearly impossible to distinguish specific effects. The recent civil asset forfeitures against North Korean financial networks, for example, netted almost $90 million. This is not an insignificant amount, especially to the operators and intermediaries within each network. Regarding the overall effect on North Korea's off-shore illicit economy, the $90 million represents a fraction of the regimes' currency reserves, which reports estimate to be approximately $3-5 billion (C4ADS, 2017; Thompson, 2017).

The case of Karl Li—the Chinese serial proliferator responsible for selling restricted goods to Iran's ballistic missile program—also illustrates the complexities of understanding the effect of disruption operations. Li remains at large, despite a $5 million reward for his arrest—the most ever offered in a proliferation case. Of course, it is unknown whether this is the result of his supposed connections to Chinese government officials or an overall lack of information permeation in China where he is based. After Mr. Li's indictment and subsequent asset forfeiture, there was little in the way of reporting in Chinese news outlets. This, of course, begs the question of whether or not information and rewards systems can be useful overseas, or in information-constrained environments, like China? Finally, there is little evidence to suggest that Mr. Li has ceased his operations. In fact, as recent as April 2018, a company affiliated with Li posted job advertisements for vacancies in his factories—suggesting that at least some of his business activities are ongoing.

Politically, opting for unilateral and extraterritorial tactics over multilateral consensus is not always the wisest choice. Surely, as others have pointed out, the benefits of multilateralism promote a shared commitment to international norms. Moreover, unilateralism can also provoke unwanted responses from needed allies. As Nye (2003, p. 105) noted, beyond being insufficient or failing, unilateral approaches will often "generate reactions"—not always in the best interest of the United States. There is emerging evidence to suggest that states are reacting that undermine both U.S. and international nonproliferation interests.

Extraterritorial use of legal and regulatory tools to disrupt illicit procurement networks requires a broad interpretation of jurisdiction. In some respects, this has had the unintended effect of reducing cooperative nonproliferation efforts. China, for example, has consistently opposed U.S. unilateral actions against its citizens. After the designation and asset forfeitures against Karl Li in 2014, a spokesman for China's Foreign Ministry chided the United States for its actions and suggested it would harm future joint

nonproliferation efforts between the two countries (Gladstone, 2014). In August 2017, when the Trump administration imposed sanctions against a number of Chinese and Russian individuals and companies responsible for facilitating North Korea's access to the international financial system, Chinese officials issued a statement that, "China opposes unilateral sanctions out of the U.N. Security Council framework, especially the 'long-arm jurisdiction' over Chinese entities and individuals exercised by any country in accordance with its domestic laws" (Morello & Whoriskey, 2017). In the case of ZTE Corp., China warned that it was "prepared to take action to protect the interests of Chinese firms" (Freifeld & Jiang, 2017; Stecklow, Freifeld, & Jiang, 2018). Perversely, countries that would stand to benefit most from cooperation and capacity building are also the most likely targets of expanded U.S. unilateral disruption efforts—potentially compounding this inherent tension in the U.S. approaches.

In 2017, the Chinese government adopted new, national-level export control laws that address many of the gaps the country has been criticized for in the past—including, establishing national enforcement mechanisms and delineating the differences between proliferation-sensitive dual-use goods and technologies. Interestingly, the text of the export control law seemingly addresses China's frustrations with foreign states' extraterritorial practices. The law articulates explicitly the right to retaliate against foreign states that take "discriminatory measures" against Chinese businesses and interests ("China prepares for new export control law," 2017). Clearly, "overuse" of unilateral tactics to disrupt illicit WMD procurement may expose U.S. economic and political interest to foreign retribution—ultimately undermining the capability to use them in the future, either through making the tools less effective or raising the political costs of their use. Furthermore, continued unilateral counterproliferation efforts may comprise existing political will to cooperate with the U.S. on future nonproliferation efforts, increases the potential for retribution by foreign states, and diminishes the utility of the tool itself—that is, the more these tools are used, the less useful they can become.

Over the last decade, U.S. policymakers have increasingly viewed sanctions and other extraterritorial actions as cost-effective, low-risk, and reproducible policy instruments while ignoring inherent hazards. These hazards become significant when extraterritorial enforcement actions are carried out without broad international consensus on the larger objectives. In effect, extraterritorial enforcement unmitigated economic coercion policies muddy the waters—making each practically indistinguishable from one another and sending confusing signals to allies.

Consequently, states have become increasingly alarmed at the expansion of U.S. extraterritoriality and politicization of the international financial system. The Obama Administration's "whisper campaign" among European banks to isolate Iran was effective because the United States made clear that pressuring Iran was part of a broader engagement strategy to achieve a diplomatic resolution to the Iranian nuclear crisis. By contrast, the Trump administration has exhibited a strong preference for unilateralism in

its foreign policy, such as its withdraw from the Joint Comprehensive Plan of Action— the 2015 agreement between the P5+1 (the United States, United Kingdom, France, China, Russia, and Germany) and Iran, which limited Iran's nuclear program in exchange for lifting international sanctions. In re-imposing financial and economic sanctions, President Trump has threatened to use secondary sanctions against European allies who do not end their business ties with Iran. This has prompted a series of political responses from European leaders, suggesting the need to insulate the European Union's economic interests and activities from American extraterritoriality.[16]

Although the reach of U.S. extraterritorial enforcement is significant, countries are not without options to resist. In recent years, several states have moved to insulate themselves against exposure to U.S. sanctions. China and Russia, for example, have each developed alternative payment systems in order to avoid dollar-dominated systems. Global companies are also seeking to limit their exposure to U.S. sanctions by exiting high-risk jurisdictions that may incur additional scrutiny by the United States— a process dubbed "de-risking." The risk that U.S. countermeasures will eventually undermine U.S. credibility and weaken extraterritorial enforcement is not insignificant.

Conclusion

In this article, we attempt to explain why the United States has increasingly resorted to extraterritorial counterproliferation enforcement efforts despite a consensus on the need for a multilateral approach to supply-side controls. We then explore the potential consequences of extraterritorial enforcement on broader nonproliferation objectives. We find that U.S. extraterritorial enforcement of counterproliferation policies is a consequence of the jurisdictional challenges posed by non-state actors, broad expansions in domestic legal interpretations of jurisdiction, and continuing gaps in global supply-side controls. While extraterritorial actions have targeted only a select number of states– namely China–it is increasingly clear that U.S. enforcement actions can jeopardize and even undermine multilateral commitments nonproliferation efforts–like UNSCR 1540.

On the surface, the U.S. approach to "going it alone" in certain hard cases of illicit procurement suggests that the Security Council's approach to governance was not without its limitations as some had originally predicted. In other words, the seemingly soft approach to governance–that is, not providing for an international enforcement

---

16

 The European Commission amended a 1996 regulation, known as the Blocking Statute, meant to insulate European companies against American secondary sanctions against Cuba, Libya, and Iran. In principle, the Blocking Statute shields against U.S. extraterritoriality by providing a legal indemnification for EU companies and individuals. That is, the statute provides a legal basis for E.U. entities to *not* comply with U.S. measures by nullifying the effect, within the EU, of any foreign decision based on extraterritorial legislation (e.g., U.S. secondary sanctions).

mechanism–did in fact open the door to coercive and extraterritorial enforcement. As a consequence, as we demonstrate, U.S. unilateral actions may be pushing states to insulate and mitigate against exposure to extraterritorial enforcement. Moreover, it is clear that U.S. policy has not fully weighed the costs of its extraterritorial enforcement actions against its impact to the 1540 regime. Given current geopolitical trends, however, it is likely that the United States will continue to leverage—or possibly expand—the use of these tools. The next comprehensive review by the 1540 committee is not until 2021. In the meantime, it will be important for the committee to explore the impact of extraterritorial enforcement on states' implementation. A richer picture may help illuminate policy options that are more consistent with the regime's approach to governance. Also, U.S. decisionmakers must reconcile the need for a greater multilateral approach to illicit WMD procurement with the need to enforce domestic rules and regulations. Instead, preference should be given to options that make use of official legal procedures while adhering to international rules and norms and should continue to reaffirm its commitments to multilateral approaches to supply-side controls by increasing outreach, capacity-building, and technical training to developing countries.

Reference list

Albright, D., Burkhard, S., Lach, A., & Stricker, A. (2018). *52 Countries Involved in Violating UNSC Resolutions on North Korea Throughout Most of 2017*. Washington, D.C.: Institute for Science and International Security.

Alexander, K. (2009). *Economic Sanctions Law and Public Policy*. London: Palgrave Macmillan.

Andreas, P. (2005). Criminalizing Consequences of Sanctions: Embargo Busting and Its Legacy. *International Studies Quarterly*, *49*, 335–360. doi:10.1111/j.0020-8833.2005.00347.x.

Arnold, A. (2017). A Resilience Framework for Understanding Illicit Nuclear Procurement Networks. *Strategic Trade Review*, *3*(4), 3–23.

Braun, C., & Chyba, C. F. (2004). Proliferation Rings: New Challenges to the Nuclear Nonproliferation Regime. *International Security*, *29*(2), 5–49. doi:10.1162/0162288042879959.

C4ADS. (2017). *The Forex Effect*. Retrieved from https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5a3292079140b73f73f92efd/1513263687907/The+Forex+Effect.pdf.

Carter, A. (2004). How to Counter WMD. *Foreign Affairs*, *83*(5), 72–85. doi:10.2307/20034068.

Chayes, A., & Chayes, A. H. (1993). On compliance. *International Organization*, *47*, 175–206. doi:10.1017/S0020818300027910.

China prepares for new export control law. (2017, August). Retrieved from https://www.worldecr.com/news/china-prepares-new-export-control-law/

Cupitt, R. T., Grillot, S., & Murayama, Y. (2001). The Determinants of Nonproliferation Export Controls: A Membership-fee Explanation. *The Nonproliferation Review*, *8*(2), 69–80. doi: 10.1080/10736700108436851.

Downs, G. W., Rocke, D. M., & Barsoom, P. N. (1996). Is the Good News about Compliance Good News about Cooperation? *International Organization*, *50*, 379–406.

doi:10.1017/S0020818300033427.
Early, B. R., Nance, M. T., & Cottrell, M. P. (2017). Global governance at the energy-security nexus: Lessons from UNSCR 1540. *Energy Research & Social Science*, *24*, 94–101. doi: http://dx.doi.org/10.1016/j.erss.2016.12.007.
Einhorn, R. J. (2006). Identifying Nuclear Aspirants and Their Pathways to the Bomb. *The Nonproliferation Review*, *13*, 491–499. doi: 10.1080/10736700601071546.
Executive Order 13382. (2005, June 28). Retrieved from https://www.state.gov/documents/organization/135435.pdf.
Freifeld, K., & Jiang, S. (2017, March 8). China's ZTE pleads guilty, settles U.S. sanctions case for nearly $900 million. *Reuters*. Retrieved from https://www.reuters.com/article/us-usa-china-zte/chinas-zte-to-pay-over-800-million-to-settle-with-u-s-over-iran-sales-source-idUSKBN16E1X1
Fuhrmann, M. (2007). Making 1540 Work: Achieving Universal Compliance with Nonproliferation Export Control Standards. *World Affairs*, *169*, 143-152. doi:10.3200/WAFS.169.3.143-152.
Fuhrmann, M. (2009). Spreading Temptation: Proliferation and Peaceful Nuclear Cooperation Agreements. *International Security*, *34*(1), 7–41. doi:10.1162/isec.2009.34.1.7.
Gladstone, R. (2014, April 30). China: Criticism of U.S. Move on Iran. *The New York Times*. Retrieved from https://www.nytimes.com/2014/05/01/world/asia/china-criticism-of-us-move-on-iran.html
Hastings, J. V. (2012). The Geography of Nuclear Proliferation Networks. *The Nonproliferation Review*, *19*, 429–450. doi:10.1080/10736700.2012.734190.
Heupel, M. (2008). Combining Hierarchical and Soft Modes of Governance: The UN Security Council's Approach to Terrorism and Weapons of Mass Destruction Proliferation after 9/11. *Cooperation and Conflict*, *43*, 7–29. doi:10.1177/0010836707082689.
Holdren, J. P. (1983). Nuclear power and nuclear weapons: the connection is dangerous. *The Bulletin of the Atomic Scientists*, *39*(1), 40–45. doi:10.1080/00963402.1983.11458937
Kelsen, H. & Trevino A. J. (1945). *General Theory of Law and State*. Cambridge, MA: Harvard University Press.
Kemp, R. S. (2017). Opening a proliferation Pandora's box: the spread of the Soviet-type gas centrifuge. *The Nonproliferation Review*, *24*, 101–127. doi:10.1080/10736700.2017.1368649.
Kemp, R. S. (2014). The Nonproliferation Emperor Has No Clothes. *International Security*, *38*(4), 39–78. doi:10.1162/ISEC_a_00159.
Kenney, M. (2007). *From Pablo to Osama: Trafficking and Terrorist Networks, Government Bureaucracies, and Competitive Adaptation*. University Park, PA: Pennsylvania State University Press.
King's College London, Project Alpha. (2016). *North Korea's Proliferation & Illicit Procurement Apparatus*. Retrieved from https://projectalpha.eu/alpha-in-depth-north-koreas-proliferation-and-illicit-procurement-apparatus/#.
Kroenig, M. (2010). *Exporting the bomb: technology transfer and the spread of nuclear weapons*. Ithaca, NY: Cornell University Press.
Miller, N. L. (2017). Why Nuclear Energy Programs Rarely Lead to Proliferation. *International Security*, *42*(2), 40–77. doi: 10.1162/ISEC_a_00293.

Monteiro, N. P., & Debs, A. (2014). The Strategic Logic of Nuclear Proliferation. *International Security*, *39*(2), 7–51. doi:10.1162/ISEC_a_00177.

Montgomery, A. H. (2005). Ringing in Proliferation: How to Dismantle an Atomic Bomb Network. *International Security*, *30*(2), 153–187. doi:10.1162/016228805775124543.

Morello, C., & Whoriskey, P. (2017, August 22). U.S. hits Chinese and Russian companies, individuals with sanctions for doing business with North Korea. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/us-sanctions-chinese-and-russian-companies-and-individuals-for-conducting-business-with-north-korea/2017/08/22/78992312-8743-11e7-961d-2f373b3977ee_story.html

Narang, V. (2016). Strategies of Nuclear Proliferation: How States Pursue the Bomb. *International Security*, *41*(3), 110–150.

Nye, J. S. (2003). *The Paradox of American Power: Why the World's Only Superpower Can't Go it Alone*. New York, NY: Oxford University Press.

Park, J., & Walsh, J. (2016). *Stopping North Korea, Inc.: Sanctions Effectiveness and Unintended Consequences*. Cambridge, MA: MIT Security Studies Program.

Perlow, G. H. (1983). Taking Peacetime Trade Sanctions to the Limit: The Soviet Pipeline Embargo. *Case Western Reserve Journal of International Law*, *15*, 253-272

Sagan, S. (1997). Why Do States Build Nuclear Weapons? Three Models in Search of a Bomb. *International Security*, *21*, 54–86.

Salisbury, D. (2019). Exploring the Use of "Third Countries" in Proliferation Networks: The Case of Malaysia. *European Journal of International Security*, 4, 101-122. doi:10.1017/eis.2018.11.

Slaughter, A.-M. (1997, September 1). The Real New World Order. *Foreign Affairs*. Retrieved from https://www.foreignaffairs.com/articles/1997-09-01/real-new-world-order

Sokolski, H. (2003, October/November). Taking Proliferation Seriously. *Policy Review, 121.* Stanford, CA: Hoover Institution.

Solensky, E., Jr. (1986). The President's International Emergency Economic Powers after Regan v. Wald: An Unchecked Proliferation of Authority Note. *Syracuse Journal of International Law and Commerce*, *12*, 125–155.

Stecklow, S., Freifeld, K., & Jiang, S. (2018, April 17). U.S. ban on sales to China's ZTE opens fresh front as tensions escalate. *Reuters*. Retrieved from https://www.reuters.com/article/us-china-zte/exclusive-u-s-bans-american-companies-from-selling-to-chinas-zte-idUSKBN1HN1P1

Stinnett, D. M., Early, B. R., Horne, C., & Karreth, J. (2011). Complying by Denying: Explaining Why States Develop Nonproliferation Export Controls. *International Studies Perspectives*, *12*, 308–326. doi:10.1111/j.1528-3585.2011.00436.x.

Swanson, A. (2018, May 25). Trump Administration Plans to Revive ZTE, Prompting Backlash. *The New York Times*. Retrieved from https://www.nytimes.com/2018/05/25/us/politics/trump-trade-zte.html

The USA PATRIOT Act, Pub. L. No. 107-56, United States (2001). Retrieved from http://purl.access.gpo.gov/GPO/LPS39935

Thompson, D. (2017). *Risky Business: A System-Level Analysis of the North Korean Proliferation Financing System*. Washington, DC: C4ADS.

Tobey, W. H. (2018). A History of United Nations Security Council Resolution 1540. In D.

Salisbury, A. Viski, & I. Stewart (Eds.), *Preventing the Proliferation of WMDs: Measuring the Success of UN Security Council Resolution 1540* (pp. 13–32). London: Palgrave Pivot.

United Nations Security Council. (2004a, April 28). *United Nations Security Council Resolution 1540 on the Non-proliferation of weapons of mass destruction*. S/RES/1540. New York: author.

United Nations Security Council. (2004b, April 28). *Press Release, Security Council Decides All States Shall Act to Prevent Proliferation of Mass Destruction Weapons*. Retrieved from https://www.un.org/press/en/2004/sc8076.doc.htm

United Nations Security Council. (2016). *Report of the Security Council Committee established pursuant to resolution 1540 (2004)*. S/2016/1038. New York: author.

United Nations Security Council. (2018). *Report of the Panel of Experts Established Pursuant to Resolution 1874*. S/2018/171. New York: author.

U.S. Department of Commerce. (2018a, April 15). *Press Release, Order Activating Suspended Denial Order Relating to Zhongxing Telecommunications Equipment Corporation and ZTE Kangxun Telecommunications LTD*. Retrieved from https://www.commerce.gov/sites/commerce.gov/files/zte_denial_order.pdf

U.S. Department of Commerce. (2018b, April 16). *Press Release, Secretary Ross Announces Activation of ZTE Denial Order in Response to Repeated False Statements to the U.S. Government*. Retrieved from https://www.commerce.gov/news/press-releases/2018/04/secretary-ross-announces-activation-zte-denial-order-response-repeated

U.S. Department of Justice. (n.d.). *U.S. Attorney's Manual, Section 279, para. B. Bank of Nova Scotia Subpoenas*. Retrieved from https://www.justice.gov/usam/criminal-resource-manual-279-subpoenas

U.S. Department of the Treasury. (2005). *Press Release, Treasury Designates Banco Delta Asia as Primary Money Laundering Concern under USA PATRIOT Act*. U.S. Department of the Treasury. Retrieved from https://www.treasury.gov/press-center/press-releases/Pages/js2720.aspx

U.S. District Court of Massachusetts. (2013, November 21). Indictment in the case of the United States of America v. Sihai Cheng. No. 13CR10332. Boston, MA: author.

U.S. District Court of New Jersey (2016, September 26). *United States of America v. Dandong Hongxiang Industrial Development Co. Ltd*. No. 2016V01954/SD/BAW/ms. Camden, NJ: author.

Williams, P. (2001). Transnational Criminal Networks. In D. Arquilla & D. Ronfeldt (Eds.), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (pp. 61-98). Arlington, VA: RAND.

Zarate, J. C. (2013). *Treasury's War: The Unleashing of a New Era of Financial Warfare*. New York, NY: PublicAffairs.